Blockchain Security Monthly Recap of May: $19.69M lost in total, down 79% from April

Beosin · Follow
5 min read · 1 day ago

It's time for another monthly security recap! According to Beosin EagleEye, a security risk monitoring, alerting and blocking platform of Beosin, in May 2023, the amount of money involved in various security incidents continued to decline for two months. **22 typical security incidents occurred in May, and the total amount of losses from various attacks was about $19.69 million, decreasing about 79% compared to April. In addition, the total amount involved in fraud reached $45.02 million, more than the amount lost in attacks.**

The largest attack of the month was the attack on Jimbos on the Arbitrum chain, with a loss of about $7.5 million. Hardware wallet-related security incidents have increased, demanding more attention from users. Frauds continued to be frequent in May, with several runaway projects involving more than $1 million.

DeFi

『10』Typical Security Incidents

№1 On May 2, Level Finance project on BSC chain was attacked and lost $1.09 million.

№2 On May 3, Never Fall on the BSC chain was attacked, with a loss of $70,000.

№3 On May 6, DEI, a stable coin launched by DEUS, was hacked and the hackers made a profit of about $6.3 million.

№4 On May 7, BFT on the BSC chain was attacked by Flash Loan, with a loss of US$270,000.

№5 On May 10, SNK on the BSC chain was attacked and hackers made a profit of $190,000 using SNK's invitation reward mechanism.

№6 On May 20, Swap-Lp on BSC chain was attacked and lost USD 1 million.

№7 On May 20, Tornado Cash was attacked and lost $1.07 million.

№8 On May 24, CS token on BSC chain was attacked and lost about $710,000.

№9 On May 24, BSC's on-chain LCT project was attacked, with a loss of about $118,000.

№10 On May 28, Jimbos on the Arbitrum chain was attacked, with a loss of about $7.5 million. The project said that if the attacker returned 90% of the funds, the attacker will not be held accountable.

Wallet/User Security

『3』Typical Security Incidents

№1 The hardware wallet imKey said it recently discovered an unofficial store selling "activated" imKey hardware wallets on its online store, which is likely to be attacked by social engineering and poses a higher risk of fraud.

№2 Security firm says Trezor T hardware wallet is vulnerable and an attacker could crack the mnemonic while physically accessing the hardware wallet.

№3 A new type of coin theft using shared charging devices to steal private keys has emerged. Fraudsters have modified KTV's shared charging devices and implanted malicious programs to steal private keys from cell phones.

Rug Pull/Crypto Scam

『6』Typical Security Incidents

№1 On May 4, XIRTAM, a project on Arbitrum, was frozen after the project owner transferred 1,909 ETH (about 3.58 million USD) to Coin Security.

№2 On May 4, a rug pull occurred on WSB Coin, a Meme coin project, involving $635,000 in funds.

№3 On May 19, a Rug Pull occurred on Swaprum, an application on Arbitrum, and the deployer made a profit of $3 million.

№4 On May 24, the team behind the blockchain financial platform Fintoch is suspected of being a Ponzi scheme and has defrauded 31.6 million USDT.

№5 On May 30, a Rug Pull occurred on the BlockGPT project, involving about $256,000 in assets.

№6 A multi-chain scam service provider called Inferno Drainer has stolen approximately $5.9 million in assets and currently has nearly 4,888 victims.

Crypto Crime

『2』Typical Security Incidents

№1 On May 20, the U.S. Department of Justice announced that a Nevada man was charged for his alleged involvement in CoinDeal, an investment fraud scheme that defrauded more than 10,000 victims of more than $45 million.

№2 In May, the U.S. Department of Justice seized up to $112 million worth of cryptocurrency from addresses associated with a cat-fishing scam.

Others

『1』Typical Security Incidents

№1 Beosin security team discovered a critical vulnerability CVE-2023–33252 in SnarkJS 0.6.11 and earlier versions of the library, alerting all zk project parties that use the SnarkJS library to update SnarkJS to version 0.7.0 to ensure security.

Extended Readin:Beosin 发现Circom 验证库漏洞CVE-2023–33252，提醒zk项目方注意相关风险

In view of the current new situation in blockchain security, 『Beosin』 concludes:

In general, **the amount involved in various blockchain security incidents continued to decline in May 2023. the total amount of losses from various attacks reached $19.69 million in May, a decline of about 79% from April.**

The amount involved in Rug Pulls exceeded that in attacks this month, and new ways of stealing coins such as using shared rechargeables to steal private keys also emerged. Hackers and scammers are gradually shifting the target of their attacks from various project parties to ordinary users. It is recommended that users must raise their anti-fraud awareness, research on projects background, and learn multiple methods to safeguard their assets. In addition, more than half of the projects attacked this month are unaudited, so it is recommended that you should always find a professional auditing company to conduct an audit before the project goes live.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan, and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML is serving 100+ institutions including Binance. You are welcome to contact us.

Contact

If you need any blockchain security services, welcome to contact us:

Official Website Beosin EagleEye Twitter Telegram LinkedIn